C L A I M S

1. A method for performing a cryptographic operation in a device (10) under the control of a security application (34), in which a cryptographic value (y) is produced in the device, by a calculation comprising at least one multiplication between two factors including a part at least of a secret key (s) associated with the device, characterized in that, a first of the two factors of the multiplication having a determined number of bits L in binary representation, the second of the two factors of the multiplication is constrained so that it comprises, in binary representation, several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L - 1 bits set to 0, and in that the multiplication is achieved by assembling binary versions of the first factor, respectively shifted in accordance with the positions of the bits set to 1 of the second factor.

2. The method as claimed in claim 1, in which the secret key (s) forms part of an asymmetric cryptographic key pair associated with the device (10).

3. The method as claimed in claim 1 or 2, in which the device (10) comprises a chip including hard-wired logic for producing the cryptographic value.

4. The method as claimed in any one of the preceding claims, in which the calculation of the cryptographic value furthermore comprises an addition or a subtraction between a pseudo-random number (r) and the result of the multiplication.

5. The method as claimed in claim 4, in which the first and second factors (s, c) and the pseudo-random number (r) are dimensioned so that the pseudo-random

number is greater than the result of the multiplication.

6. The method as claimed in claim 5, in which the number of bits set to 1 of the second factor is chosen at most equal to the largest integer less than or equal to s_1/L, where s_1 is a predefined threshold less than the number of bits of the pseudo-random number (r) in binary representation.

7. The method as claimed in any one of the preceding claims, in which the two factors of the multiplication include, as well as said part of the secret key (s), a number (c) provided to the device by the security application executed outside the device.

8. The method as claimed in any one of claims 1 to 6, in which the two factors of the multiplication include, as well as said secret key (s), a number (c) provided by the device.

9. The method as claimed in any one of the preceding claims, in which said part of the secret key (s) is said first factor of the multiplication.

10. The method as claimed in claim 9, in which said binary versions are disposed in respective intervals of like size in bits, said size corresponding to the total size of a usable space, divided by the number of bits set to 1 of the second factor of the multiplication, each binary version being placed in its respective interval as a function of a shift in accordance with the positions of the bits set to 1 of the second factor.

11. The method as claimed in any one of claims 1 to 8, in which said part of the secret key (s) is the second factor of the multiplication.

12. The method as claimed in claim 11, in which the secret key (s) is stored in a memory support of the device by coding the positions of its bits set to 1.

13. The method as claimed in any one of claims 11 to 12, in which the secret key (s) is stored in a memory support (16) of the device by coding numbers of bits separating respectively lower bounds of intervals of (S-1)/(n-1) bits and lower bounds of blocks of bits allotted to the first factor (c) of the multiplication and each disposed in the associated intervals, S being the number of bits of the secret key and n the number of bits set to 1 of the secret key.

14. The method as claimed in any one of claims 11 to 12, in which the secret key (s) is stored in a memory support (16) of the device by coding numbers of bits, each representative of the number of bits separating two blocks of successive bits allotted to the first factor (c) of the multiplication.

15. The method as claimed in any one of the preceding claims, in which the cryptographic value (y) is produced so as to authenticate the device in a transaction with the security application executed outside the device.

16. The method as claimed in any one of claims 1 to 14, in which the cryptographic value (y) is produced in the guise of electronic signature.

17. A device with cryptographic function, comprising means (24) of interfacing with a security application (34) and means of calculation (12, 22, 26) for producing a cryptographic value (y), the means of calculation comprising means of multiplication (22) between two factors including a part at least of a

secret key (s) associated with the device, characterized in that, a first of the two factors of the multiplication having a determined number of bits L in binary representation, and the second of the two factors of the multiplication being constrained so that it comprises, in binary representation, several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L - 1 bits set to 0, the multiplication means comprise means for assembling binary versions of the first factor, respectively shifted in accordance with the positions of the bits set to 1 of the second factor.

18. The device as claimed in claim 17, furthermore comprising means (12) of generating a pseudo-random number (r), the means of calculation comprising means (26) for adding the result of the multiplication to or subtracting it from said pseudo-random number.

19. The device as claimed in claim 18, in which the first and second factors (s, c) and the pseudo-random number (r) are dimensioned so that the pseudo-random number is greater than the result of the multiplication.

20. The device as claimed in any one of claims 17 to 19, in which the means (12, 22, 26) of calculation are embodied as hard-wired logic.

21. The device as claimed in any one of claims 17 to 20, in which said part of the secret key (s) is the first factor of the multiplication.

22. The device as claimed in any one of claims 17 to 20, in which said part of the secret key (s) is the second factor of the multiplication.

23. The device as claimed in claim 22, furthermore comprising a memory (16) adapted for storing data for coding the positions of the bits set to 1 of the secret key (s).